Lecture 5.

Let F be a field. We consider the ring of polynomials $F[t]$.

Theorem. An arbitrary nontrivial ideal of $F[t]$ is of the type $(f(t))$, $\deg f(t) \geq 1$.

Proof. Let I be an ideal of $F[t]$. If I contains a nonzero constant $\alpha \in F$ then I contains $1 = \alpha \cdot \frac{1}{\alpha}$ and therefore $I = F[t]$.

We will assume that I does not contain nonzero constant, so the degree of an arbitrary nonzero element from I is ≥ 1.

Let $f(t)$ be a nonzero element from I

of the smallest degree. Again we make use of the fact that every nonempty subset of $N = \{1, 2, \dots\}$ contains a minimal element.

We will show that every nonzero element from I is divisible by $f(t)$.

Indeed, let $h(t) \in I$. There exist polynomials $q(t)$ and $r(t)$, $\deg r(t) < \deg f(t)$ such that

$$h(t) = f(t)\, q(t) + r(t).$$

But $r(t) = h(t) - f(t)\, q(t) \in I$. Since $f(t)$ has the smallest degree among <u>nonzero</u> elements of I it follows that $r(t) = 0$.

We claim that $I = (f(t))$. Indeed, $f(t) \in I$ implies $(f(t)) = f(t)F[t] \subseteq I$. On the other hand every element of I is a multiple of $f(t)$, hence $I \subseteq f(t)F[t]$. This completes the proof of the theorem. $\square$

<u>Exercise</u>. Prove that an arbitrary nontrivial ideal of $\mathbb{Z}$ is of the type $n\mathbb{Z}$, $n \geq 2$.

<u>Hint</u>: argue as in the proof of the Theorem.

<u>Remark.</u> Let $m, n \geq 1$. Then $n\mathbb{Z} \subseteq m\mathbb{Z}$ if and only if $m \mid n$.

Indeed, if $n = mk$ then $n\mathbb{Z} = mk\mathbb{Z} \subseteq m\mathbb{Z}$. On the other hand, if $n\mathbb{Z} \subseteq m\mathbb{Z}$ then $n \in m\mathbb{Z}$, hence n is a multiple of m.

Maximal ideals.

Let R be a commutative ring with $\mathbb{1}$

Def. An ideal $I \lhd R$ is said to be a maximal ideal if

(1) I is smaller, than R, $I \subsetneq R$;

(2) there is no ideal $J \lhd R$ that lies strictly between I and R (that is $I \subsetneq J \subsetneq R$).

Example. Let p be a prime number. Then $p\mathbb{Z}$ is a maximal ideal of $\mathbb{Z}$.

Indeed, suppose that $J \lhd \mathbb{Z}$ and

$$p\mathbb{Z} \subseteq J \subseteq \mathbb{Z}.$$

By the Exercise above $J = n\mathbb{Z}$. By the Remark $p\mathbb{Z} \subseteq n\mathbb{Z}$ implies that n is a divisor of p, hence $n = 1$ or p. If $n = p$ then

$p\mathbb{Z} = J$. If $n=1$ then $J = \mathbb{Z}$.

<u>Theorem</u>. Let R be a commutative ring with $\mathbb{1}$. Let I be an ideal of R. The following conditions are equivalent:

(1) the factor ring R/I is a field;

(2) the ideal I is maximal.

<u>Proof</u>. (1) $\Rightarrow$ (2). Suppose that the factor ring R/I is a field. Our aim is to prove that the ideal I is maximal.

Let $a \in R \setminus I$, hence $a+I$ is a nonzero element of the field R/I. A nonzero element of a field has an inverse. Let $b+I \in R/I$ be the inverse of $a+I$,

$$(a+I)(b+I) = ab+I = 1+I.$$

Now suppose that the ideal I is not maximal and there exists an ideal $J \triangleleft R$ such that $I \subsetneq J \subsetneq R$. Choose an element $a \in J \setminus I$.

We have seen above that there exists an element $b \in R$ such that

$$(a+I)(b+I) = ab + I = 1 + I.$$

Hence there exists an element $c \in I$ such that

$$ab = 1 + c.$$

The element ab lies in J because $a \in J$. The element c lies in J because $c \in I$ and $I \subset J$. Therefore

$$1 = ab - c \in J,$$

which implies $J = R$, a contradiction.

(2) $\Rightarrow$ (1). Now suppose that the ideal I is

maximal. Our aim is to show that the factor-ring R/I is a field. Choose a nonzero element $a+I \in R/I$, $a \in R \setminus I$. We have to show that the element $a+I$ has an inverse.

Consider $J = I + aR = \{c + ax \mid c \in I, x \in R\}$. It is easy to see that J is an ideal of R.

The ideal J is strictly bigger than I. Indeed, $a \in J \setminus I$.

Since the ideal I is maximal it follows that $J = R$. In particular there exist elements $c \in I$, $x \in R$ such that

$$c + ax = 1.$$

Now $(a+I)(x+I) = ax + I = 1 \underbrace{- c + I}_{= I} = 1 + I,$

so $x+I=(a+I)^{-1}$.

We proved that an arbitrary nonzero element of R/I has an inverse. In other words R/I is a field. $\blacksquare$

<u>Question</u>. Let F be a field and let $f(t)$ be a polynomial over F. When is the ideal $(f(t))$ maximal?

<u>Def</u>. A polynomial $f(t)$ is called <u>irreducible</u> if

(1) $\deg f(t) \geqslant 1$, so $f(t)$ is not a constant,

(2) $f(t)$ can not be represented as

$$f(t) = f_1(t) f_2(t)\ ; \ \deg f_1(t), \deg f_2(t) \geqslant 1.$$

<u>Example</u>. Any polynomial $t-\alpha$, $\alpha\in F$, is irreducible.

<u>Proposition.</u> Let $f(t)$ be a polynomial of degree ≥ 1. The following conditions are equivalent:

(1) the ideal $(f(t))$ is maximal,

(2) the polynomial $f(t)$ is irreducible.

<u>Proof.</u> (1) $\Rightarrow$ (2). Suppose that the ideal $(f(t))$ is maximal, but ... $f(t) = f_1(t)\, f_2(t)$;

$\deg f_1(t), \deg f_2(t) \geq 1$.

The ideal $(f(t))$ is strictly contained in the ideal $(f_1(t))$ and $(f_1(t)) \neq F[t]$,

so $\quad (f(t)) \subsetneqq (f_1(t)) \subsetneqq F[t]$.

This contradicts maximality of the ideal $(f(t))$.

(2) $\Rightarrow$ (1). Suppose that the polynomial $f(t)$ is irreducible. We need to show that the ideal $(f(t))$ is maximal. Suppose the contrary: $(f(t)) \subsetneqq J \subsetneqq F[t]$, $J \triangleleft F[t]$.

We showed above that every ideal of $F[t]$ is of the type $(g(t))$, where $g(t)$ is some polynomial. Let $J = (g(t))$. The polynomial $g(t)$ is not a nonzero constant, otherwise $J = F[t]$. Hence

$\deg g(t) \geq 1$.

The inclusion $f(t) \in (g(t))$ means that $f(t)$ is a multiple of $g(t)$,

$$f(t) = g(t)\, h(t).$$

Since the polynomial $f(t)$ is irreducible it follows that $\deg h(t) = 0$, $h(t) = \alpha$ is a nonzero constant. But in this case $(f(t)) = (f(t)\cdot\alpha) = (g(t)) = J$, the contradiction. $\downarrow$

Given a polynomial $f(t)$ how can we decide if $f(t)$ is irreducible or not?

<u>Proposition</u>. Let $\deg f(t) = 2$ or 3. Then $f(t)$ is irreducible (over the field F) if and only if it does not have roots in F.

<u>Proof</u>. If $f(t)$ has a root $\alpha \in F$ then $f(t)$ is divisibly by $t-\alpha$, hence it is not irreducible.

Suppose that the polynomial $f(t)$ is not irreducible, $f(t) = f_1(t) \cdot f_2(t)$. Then $\deg f_1(t) + \deg f_2(t) = \deg f(t) = 2$ or 3. Hence the smaller number of $\deg f_1(t)$, $\deg f_2(t)$ is equal to 1. Let $\deg f_1(t) = 1$, $f_1(t) = \alpha t + \beta$, $\alpha \neq 0$. Then $-\beta/\alpha$ is a root of the polynomial $f(t)$. $\downarrow$

Example. The polynomial $t^2 - 3$ is irreducible over the field $\mathbb{Z}(5)$.

Indeed, $\mathbb{Z}(5) = \{0, 1, 2, 3, 4\}$. The squares of these elements are equal to:

$$0, 1, 4, 4, 1.$$

We see that 3 is not a square. Hence the polynomial $t^3 - 3$ does not have roots in $\mathbb{Z}(5)$.

<u>Example.</u> The polynomial t^2+t+1 is irreducible over $\mathbb{Z}(2)$.

Indeed, $\mathbb{Z}(2)=\{0,1\}$. We have $f(0)=1$, $f(1)=1$. Hence $f(t)=t^2+t+1$ does not have roots in $\mathbb{Z}(2)$. $\downarrow$

<u>Example.</u> The polynomial t^3+t+1 is irreducible over $\mathbb{Z}(2)$.

The proof is the same as above.

The factor-rings $\mathbb{Z}(5)[t]/(t^2-3)$, $\mathbb{Z}(2)[t]/(t^2+t+1)$, $\mathbb{Z}(2)[t]/(t^3+t+1)$ are fields.

What are their orders?

Let F be a field ~~F be a field~~, $f(t) = t^d + \cdots + a_0$, a polynomial of degree d, the leading coefficient $= 1$.

<u>Lemma</u>. Every coset of the ideal $(f(t))$ in $F[t]$ is of the type $g(t) + (f(t))$, $\deg g(t) < d$. If $g(t), h(t)$ are different polynomials of degree $< d$ then the cosets $g(t) + (f(t))$, $h(t) + (f(t))$ are different.

In other words,

$$F[t]/(f(t)) \xleftrightarrow{1-1} \text{polynomials of degree} < d$$

<u>Proof</u>. Let C be a coset of the ideal $(f(t))$ in $F[t]$. We claim that C contains a polynomial of degree $< d$. Indeed, choose

a nonzero element $p(t) \in C$ and divide $p(t)$ by $f(t)$ with a remainder:

$$p(t) = f(t)\,q(t) + r(t), \ \deg r(t) < d.$$

The polynomial $r(t)$ lies in the coset C. Hence $C = r(t) + (f(t))$.

If $g(t), h(t)$ are both polynomials of degrees $< d$ and $g(t) + (f(t)) = h(t) + (f(t))$ then $g(t) - h(t)$ is divisible by $f(t)$. Since $\deg(g(t) - h(t)) < \deg f(t)$ it follows that $g(t) - h(t) = 0$. $\top$

<u>Corollary.</u> If $F = \mathbb{Z}(p)$ then $F[t]/(f(t))$ contains p^d elements.

<u>Proof.</u> The number of elements in $F[t]/(f(t))$ is equal to the number of polynomials of

degree $< d$

$$a_0 + a_1 t + \cdots + a_{d-1} t^{d-1}$$

For each of $a_0, a_1, \ldots, a_{d-1}$ there are p candidates from $\mathbb{Z}(p)$. Hence

$$\# = p^d.$$

<u>Corollary.</u> $\mathbb{Z}(5)[t]/(t^2-3)$, $\mathbb{Z}(2)[t]/(t^2+t+1)$, $\mathbb{Z}(2)[t]/(t^3+t+1)$ have orders $25, 4, 8$ respectively.